In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer using a secure connection via an intermediate computer in a telecommunication network, comprising:

the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish [[a]] the secure connection between the first computer and the second computer via the intermediate computer,

the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,

sending the secure message, using the secure connection, containing the first unique identity and the first destination address from the first computer to the intermediate computer,

the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer,

the intermediate computer substituting the first destination address with the second destination address to the second computer,

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection, and

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the

first computer and the intermediate computer, the unique identity.

8. (Previously presented) The method of claim 1 wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the

method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:
a first computer, a second computer and an intermediate computer,
means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and an IP destination address of the second computer as a second end point,
the first and the second computers having means for performing an IPSec processing,
the intermediate computer having translation means for using translation tables to perform IPsec and IKE translation and for changing a destination address of the intermediate computer of a secure message, containing a unique identity, to a destination address of the second computer without decrypting the secure message, and
the intermediate computer having means for using the unique identity when forwarding the secure message received from the first computer to the second computer in the security association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:
a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
a negotiating and key exchanging module between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and

the intermediate computer performing translation between destination addresses and secure identities for forwarding a secure message, containing a unique identity, received from the first computer and using the unique identity when forwarding the secure message to the second computer in the secure connection without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection.

28. (Original) The method of claim 1 wherein the method further comprises the intermediate computer substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the second computer.

29. (Original) The method of claim 1 wherein the packets between the first computer and intermediate computers are sent using a UDP protocol.